PCT / IB 00 / 00319
13. 04. 00

STATE PF ISRAEL

This is to certify that annexed bereto is a true copy of the documents as originally deposited with the patent application particulars of which are specified on the first page of the annex.

זאת לתעודה כי רצופים בזה העתקים נכונים של המסמכים שהופקדו לכתחילה עם הבקשה לפטנט לפי הפרטים הרשומים בעמוד הראשון של הנספח.

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

This 14-03-2000 היום

מ. לסרי
ממונה על הבוחנים

רשם הפטנטים
Registrar of Patents

חוק הפטנטים, התשכ"ז–1967
PATENTS LAW, 5727–1967

בקשה לפטנט
Application for Patent

לשימוש הלשכה
For Office Use

מספר: Number	125720
תאריך: Date	25-02-1999
הוקדם/נדחה Ante/Post-dated	

אני, (שם המבקש, מענו – ולגבי גוף מאוגד – מקום התאגדותו)
I (Name and address of applicant, and, in case of a body corporate, place of incorporation)

יצחק לבטון
אז"ל 5
ירושלים

ISAAC J. LABATON
ETZEL, 5
JERUSALEM

בעל אמצאה מכח אנקולון בע"מ ENCOTONE LTD שמה הוא:
Owner, by virtue of of an invention, the title of which is:

(בעברית) (Hebrew) שיטה לאישור בעלות העסקות מרחוק בטלפון.

(באנגלית) (English) A Method for Certification of over-the-phone Transactions

מבקש בזאת כי ינתן לי עליה פטנט.
hereby apply for a patent to be granted to me in respect thereof.

* בקשת חלוקה – Application for Division	* בקשת פטנט מוסף – Application for Patent of Addition	* דרישת דין קדימה Priority Claim		
מבקשת פטנט from Application	* לבקשה/לפטנט to Patent/Appl.	מספר/סימן Number/Mark	תאריך Date	מדינת האיגוד Convention Country
No. מס'	No. מס'			
dated מיום	dated מיום			

* יפוי כח: כללי/מיוחד – רצוף בזה / עוד יוגש
P.O.A.: general / specific – attached / to be filed later –

Has been filed in case הוגש בעניין

המען למסירת הודעות ומסמכים בישראל
Address for Service in Israel
אנקולון בע"מ ENCOTONE LTD
ת.ד. 45074 המרכבה 8, 45074 P.O.B.
ירושלים 91450 HAMARPE 8, JERUSALEM

חתימת המבקש
Signature of Applicant

היום 25 בחודש פברואר שנת 1999
This 25th of February 1999

לשימוש הלשכה
For Office Use

* זה, כשהוא מוטבע בחותם לשכת הפטנטים ומושלם במספר ובתאריך ההגשה, הינו אישור להגשת הבקשה שפרטיה רשומים לעיל.

A method for Certification of Over-the-phone Transactions

Isaac J. Labaton

Technical Field

The present invention relates, generally, to the identification of persons which sustain transactions Over-the- phone, as well as the certification of the pertinent transaction data.

Background Art and Technical Problems

Over-the-phone transactions in general includes the Tele-Bank services, or Bank over-the phone, the transactions given to brokerage houses through the phone, as well as buying and selling over-the-phone, mostly based on Credit card transactions.

These transaction have security problems , like the Identification of the parties and the certification of the transaction data.

There is a wide acceptation by the public, world wide, about the potential of the methodology to complete transactions which is referred as e-commerce.
One of the factors which support the potential of the said methodology to complete transactions are the security aspects: the customer can be identified with security , as well as the pertinent transaction data can be digitally signed, by using a digital Certificate, previously delivered to the customer by one of the certification authorities.
Examples of the said certification authorities servicing companies are Verisign and Entrust both USA companies selling digital certificates.

There is also agreement that the e-commerce has restricted accessibility: In order to perform an e-commerce transaction the customer needs a personal computer or a similar device , and the necessary skills for managing himself in the Internet.

Lately there are very serious intents, by big corporations, to develop technology for expanding the benefits of the e-commerce to people which have no a PC, or the capability to use one. This emerging technology and trend is referred as Voice-Browsers. A Voice Browser is software running in a PC or alike, which can

"understand" voice instructions by means of Speech recognition technologies, and "read out" text using Text to speech technologies.

One of the aims is to enable people to perform Internet transactions from any phone, uttering instructions and hearing responses through the phone, any phone.
In other words , several companies are developing servers which are connected to the Internet and to the PSTN, and which can bridge between them.
This will open the e-commerce to a 5 billion people which today have phones and fill comfortable with that devices.
Nevertheless, there is a big technical restriction imposed by the present technology and methodology, which limit the security of the e-commerce, when the customer is in the phone. Technically, the Certification methodology in use by the Certification authorities companies, can not work through a regular phone.
The need of an additional piece of hardware connected to the phone (like an Chip Card reader), restrict the use of certain phones (i.e.; public phones) and it is not convenient.
To change the phone sets for new and more intelligent sets is a far away and very costly possibility.

Therefore, there is a need for a new methodology and devices, which will enable the Identification and Certification of the Over-the-phone transactions in general and the e-commerce transaction through the phone in particular.

Summary of the Invention

The method of this invention is designed for solving the identification problems of persons which use the phone in order to perform transactions, adapting the PC based Certification technology and methods to regular phones.

The method consists of
1.-the use, by the caller, of a small device able
1.1 to compute a fresh ,new ,dynamic and secure identification code and
1.2 to encode this dynamic and secure identification code to sound, whereas this sound carrying the dynamic and secure identification code, is referred as the Acoustic Signature
2 to place a call to the service provider and to send , during the session the said Acoustic Signature through the phone set microphone, whereas this sound is converted to an electromagnetic signal and is transmitted through the PSTN to the Service Provider as any caller's utterance is and

3 whereas, at the service provider facilities ,such Acoustic Signature is digitized (i.e.: creating a file) and
4 whereas a reverse encoding process (de-codification) is applied to such digitized Acoustic Signature recuperating the dynamic and secure identification code and
5 whereas such string of digits referred as dynamic and secure identification code is transmitted to a third party, referred herebelow as the Notarial Certificator Server and
6 whereas the Notarial Certificator Server interprets and decrypts the dynamic and secure identification code identifying the specific small device
7 and whereas a database is queried in order to find out who is the owner of such small device that generated the Acoustic Signature and
8 whereas once the small device owner was identified, the Notarial Certificator Server emulates a virtual owner's PC sending a regular digital certificate previously received from an existent certification authority company and stored,.

A variation of this method consists of : wherever a person (a Caller) would like to perform a secure Internet transaction through a regular phone , he should use a small hand-held device, which was issued to him previously, and is associated with the caller (the caller is the legitimate Owner of the hand-held device), whereas the small hand-held device is able
1.- to identify the authorized and legitimate device's Owner by requesting a Personal Identification number , known only by him and
1.1 to compute a fresh ,new ,dynamic and secure identification code every time the small hand-held device is actuated and
1.2 to accept transaction data (i.e.: transaction amount, type of transaction, account number, destination phone number, etc) locally entered and , preferable, to encrypt such transaction data and
1.3 to encode this dynamic and secure identification code and the encrypted transaction data to sound, whereas this sound, carrying the dynamic and secure identification code and the encrypted transaction data , is referred as the Acoustic Signature
2 and whereas the Caller places a call to the service provider and sends, during the calling session, the said Acoustic Signature through the phone set's microphone, whereas this sound is converted to an electromagnetic signal at the microphone and is transmitted through the PSTN to the Service Provider as any caller's utterance is, and
3 whereas, at the service provider facilities ,such Acoustic Signature is digitized (i.e.: creating a file) and
4 whereas a reverse encoding process (de-codification) is applied to such digitized Acoustic Signature recuperating the said dynamic and secure identification code and the encrypted transaction data and
5 whereas such string of digits referred as dynamic and secure identification code and the encrypted transaction data are transmitted to a third party, referred here-below as the Voice-Notarial Certificator Server and

6 whereas the Voice-Notarial Certificator Server interprets and decrypts the dynamic and secure identification code identifying the specific small hand-held device and the encrypted transaction data sent
7 and whereas a database is queried in order to find out who is the owner of such small device that generated the Acoustic Signature and
whereas once the small device owner was identified and the data decrypted, the Voice Notarial Certificator Server sends a digital document , referred as Notarial Certificate to the service provider certifying the Identity of the Caller and the data entered on the small device.

A more detailed description of the method of this patent consists of:
1 issuing to each person , which desires to perform secure and certified Internet transaction from a regular phone, as a one time set-up procedure, a small hand-held device, and, fulfilling the procedure to request a certificate from an accepted Certification Authority, as such as Verisign or other, in a way that the Voice –Notarial Certificator Server will be able to generates digital documents certified by using the Certification authority procedures and specific keys, given to the person and stored in the Voice –Notarial Certificator service database.
2 Whereas the small hand-held device requests a PIN to be actuated, and whereas the first , given, manufactures' PIN is only valid, and necessary for changing such a first PIN for a new, only know to the legitimate owner, PIN, and whereas such manufacturer's PIN is given to the person only after having checking his identity carefully once and forever, and whereas, after having changing the PIN for a new one, due to the fact that the small hand-held device permits a limited number of consecutive wrong PINs (say 3 or 10) before auto locking itself, only the legitimate owner has the capability to actuate such small hand-held device, and

3 wherever a person (a Caller) would like to perform a secure Internet transaction through a regular phone , he should use his small hand-held device, which was associated with the caller at one of the Voice –Notarial Certificator service databases, whereas the small hand-held device is able
4 to identify the authorized and legitimate device's Owner by requesting the Personal Identification Number and
4.1 to compute a secure identification code every time the small hand-held device is actuated and
4.2 to accept transaction data (i.e.: transaction amount, type of transaction, account number, destination phone number, etc) locally entered by the caller at the time of the transaction by means of the key-pad of the small hand-held device and , preferable, to encrypt such transaction data and
4.3 to encode this secure identification code and the encrypted transaction data to sound, whereas this sound, carrying the dynamic and secure

identification code and the encrypted transaction data , is referred as the Acoustic Signature

5 and whereas the Caller places a call to the service provider and sends, during the calling session, the said Acoustic Signature through the phone set's microphone, whereas this sound is converted to an electromagnetic signal at the microphone and is transmitted through the PSTN to the Service Provider as any caller's utterance is, and

6 whereas, at the service provider facilities ,such Acoustic Signature is digitized (i.e.: creating a file) and

7 whereas the reverse of the encoding process carried on in the small hand-held device , referred as de-encoding process (de-codification) is applied to such file containing the digitized Acoustic Signature recuperating the said dynamic and secure identification code and the encrypted transaction data and

8 whereas such string of digits referred as dynamic and secure identification code and the encrypted transaction data is transmitted to a third party, referred here-below as the Voice-Notarial Certificator service and

9 whereas the Voice-Notarial Certificator service's Server interprets ,decrypts or re-compute and compare, the dynamic and secure identification code, identifying the specific small hand-held device and the encrypted transaction data sent

10 and whereas a database is queried in order to find out who is the owner of such small device that generated the Acoustic Signature, or in another words , to whom such small device was associated and

11 whereas once the small device owner was identified and the transaction data decrypted, the Voice Notarial Certificator Server queries a database where the personal keys of the small hand-held device legitimate owner are stored, which can be the same said database where the small hand-held device is associated to the Owner, or a different one, and prepares a signed document according with the procedures recommended and in use by the certification authorities , emulating the legitimate small device Owner as he will be sited in front of a PC with the personal keys once delivered by the Certification authority and prepares the document certification in a way such that the caller is in the phone and the service provider server receives a secure digital document according to the usage of the certification authorities, and in use standards.

Detailed Description of Preferred Exemplary implementations of the method of this invention

A preferred variation of the method of this invention is as follows:

1 issuing to each person , which desires to perform secure and certified Internet transaction from a regular phone, as a one-time set-up procedure, a small hand-held device, and, fulfilling the procedure to request a certificate from an accepted Certification Authority, as such as Verisign or other, in a way that

the Voice –Notarial Certificator Server will be able, upon the person request as specified below, to generate digital documents certified by using the Certification authority procedures and specific keys, given to the person and stored in the Voice –Notarial Certificator service database.

2 Whereas the small hand-held device requests a PIN to be actuated, and whereas the first , given, manufactures' PIN is only valid, and necessary for changing such a first PIN for a new, only know to the legitimate owner, PIN, and whereas such manufacturer's PIN is given to the person only after having checking his identity carefully once and forever, and whereas after having changing the PIN for a new one, due to the fact that the small hand-held device permits a limited number of consecutive wrong PINs (say 3 or 10) before auto locking itself, only the legitimate owner has the capability to actuate such small hand-held device, and

3 wherever a person (a Caller) would like to perform a secure Internet transaction through a regular phone , he should use his small hand-held device, which was associated with the caller at one of the Voice –Notarial Certificator service databases, whereas the small hand-held device is able

4 to identify the authorized and legitimate device's Owner by requesting the Personal Identification Number and

4.1 to compute a secure identification code every time the small hand-held device is actuated and

4.2 to accept transaction data (i.e.: transaction amount, type of transaction, account number, destination phone number, etc) locally entered by the caller at the time of the transaction by means of the key-pad of the small hand-held device and , preferable, to encrypt such transaction data and

4.3 to encode this secure identification code and the encrypted transaction data to sound, whereas this sound, carrying the dynamic and secure identification code and the encrypted transaction data , is referred as the Acoustic Signature

5 and whereas the Caller places a call to the service provider and sends, during the calling session, the said Acoustic Signature through the phone set's microphone, whereas this sound is converted to an electromagnetic signal at the microphone and is transmitted through the PSTN to the Service Provider as any caller's utterance is, and

6 whereas, at the service provider facilities ,such Acoustic Signature is digitized (i.e.: creating a file) and

7 whereas the reverse of the encoding process carried on in the small hand-held device , referred as de-encoding process (de-codification) is applied to such file containing the digitized Acoustic Signature recuperating the said dynamic and secure identification code and the encrypted transaction data and

8 whereas such string of digits referred as dynamic and secure identification code and the encrypted transaction data is encrypted and/ or Hashed , preferable, according to the standards and use of the e-commerce Certification authorities,(here-below referred as Client Query) and whereas

such Client Query is transmitted to a third party, referred here-below as the Voice-Notarial Certificator service and

9 whereas the Voice-Notarial Certificator service's Server decrypts and re checks the Client Query recuperating the dynamic and secure identification code and transaction data and

10 interprets ,decrypts or re-compute and compare, the dynamic and secure identification code, identifying the specific small hand-held device and decrypts the encrypted transaction data sent

11 and whereas a database is queried in order to find out who is the owner of such small device that generated the Acoustic Signature, or in another words to whom such small device was associated and

12 whereas once the small device owner was identified and the transaction data decrypted, the Voice Notarial Certificator Server queries a database where the personal keys of the small hand-held device's legitimate owner are stored, which can be the same said database where the small hand-held device is associated to the Owner, or a different one,

13 and whereas the Voice Notarial Certificator Server prepares a signed document according with the procedures recommended and in use by the certification authorities , emulating the legitimate small device Owner as he would be sited in front of a PC with the personal keys previously delivered by the Certification authority and prepares the document certification

whereas this method results in a in a way of bridging the PSTN with the Internet such that , as a summary, the caller is actually in the phone and the service provider server receives a secure digital document according to the usage of the e-commerce certification authorities, in use ,standards.

A preferred variation of the method of this invention , for remote, Credit Card based, over-the-phone transactions consists of:

1. issuing to each person (the customer), which desires to perform remote Credit Card based transactions from a regular phone with signature-on-file, as a one time set-up procedure, a small hand-held device, and, obtaining from such person, an authorization to use one or several of his credit cards for paying transactions according with the procedures stated here-below, in a way that the Voice –Notarial Certificator Server will be able, upon the person request , as specified below, to stamp a digital signature on documents
2. and obtaining from such customer, also, as a one time procedure, all the necessary data, including name of the customer, Credit card numbers, expiration dates, and, if requested, the digital signature of the customer and/or the facsimile of the hand-written signature of the customer to be stamped and used as described below
3. Whereas the small hand-held device requests a PIN to be actuated, and preferable, whereas the first , given, manufactures' PIN is only valid, and necessary for changing such a first PIN for a new, only know to the

legitimate owner, PIN, and whereas such manufacturer's PIN is given to the person only after having checking his identity carefully once and forever, and whereas, after having changing the PIN for a new one, due to the fact that the small hand-held device allows a limited number of consecutive wrong PINs (say 3 or 10) before auto locking itself, only the legitimate owner has the capability to actuate such small hand-held device, and

4. wherever the person (the customer) would like to perform a secure Credit Card transaction through a regular phone , he should use his small hand-held device, which was associated with the customer on one of the Voice – Notarial Certificator service databases, whereas the small hand-held device is able

5. to identify the authorized and legitimate device's Owner (the customer) by requesting the Personal Identification Number and
5.1 to compute a fresh secure identification code every time the small hand-held device is actuated and
5.2 to accept transaction data (i.e.: transaction amount, selection of the Credit Card, etc) locally entered by the customer at the time of the transaction by means of the key-pad of the small hand-held device and , preferable, to encrypt such transaction data and
5.3 to encode this secure identification code and the encrypted transaction data to sound, whereas this sound, carrying the dynamic and secure identification code and the encrypted transaction data , is referred as the Acoustic Signature

5 and whereas the Customer places a call to the service provider and sends, during the calling session, the said Acoustic Signature through the phone set's microphone, whereas this sound is converted to an electromagnetic signal at the microphone and is transmitted through the PSTN to the Service Provider as any customer's utterance is, and

6 whereas, at the service provider facilities ,such Acoustic Signature is digitized (i.e.: creating a file) and

7 whereas the reverse of the encoding process carried on in the small hand-held device , referred as de-encoding process (de-codification) is applied to such file containing the digitized Acoustic Signature recuperating the said dynamic and secure identification code and the encrypted transaction data and

8 whereas such string of digits referred as dynamic and secure identification code and the encrypted transaction data are encrypted and/ or Hashed , preferable, according to the standards and usage of the e-commerce Certification authorities,(whereas such encrypted string is referred here-below referred as Client Query) and whereas such Client Query is transmitted to a third party, referred here-below as the Voice-Notarial Certificator service over data lines and

9 whereas the Voice-Notarial Certificator service's Server decrypts and/or re checks the integrity and validity of the Client Query recuperating, eventually, the dynamic and secure identification code and transaction data and

10 interprets ,decrypts or re-compute and compare, the dynamic and secure identification code, identifying the specific small hand-held device and decrypts the encrypted transaction data sent
11 and whereas a database is queried in order to find out who is the owner of such small device that generated the Acoustic Signature, or in another words to whom such small device was associated with and
12 whereas once the small device owner was identified and the transaction data decrypted, the Voice Notarial Certificator Server queries a database where the Credit Card account numbers associated with such small hand-held device or/and customer are stored which can be the same said database where the small hand-held device is associated to the Owner, or a different one, and
13 whereas the Voice Notarial Certificator service queries the relevant Credit card company for obtaining authorization of the payment, directly or through a point-of sale machine, and/or through any of the companies who serves as clearing houses for Credit card transactions
14 and ,eventually , having obtained the respective authorization from the relevant credit card company
15 the Voice Notarial Certificator Server prepares a digitally signed document, with the necessary data for the complexion of the Credit Card based transaction, including name of the customer, Credit card number, amount , expiration date, and, if requested, the digital signature of the customer and/or the digital certificate generated by the Voice Transaction Notarial service, and/or the facsimile of the hand-written signature of the customer, in order to fulfill the credit card companies request of signature-on-file,
16 and whereas the document is send to the service provider over data lines

whereas this method results in a in a way of supporting the provision of signature on file for remote credit card transaction performd through the phone.

A further preferred variation of the method of this invention , for remote, Credit Card based, over-the-Internet ,transactions originated through the phone and referred as Voice-commerce transactions consists of:

1. issuing to each person (the customer), which desires to perform remote Credit Card based over-the-Internet transactions from a regular phone with security, as a one time set-up procedure, a small hand-held device, and, obtaining from such person, an authorization to use one or several of his credit cards for paying transactions according with the procedures stated here-below, in a way that a third party, referred as the Voice –Notarial Certificator Server, will be able, upon the person request , as specified below, to stamp a digital signature on documents according with the electronic-commerce standards (e-commerce)

6. and obtaining from such customer, also, as a one time procedure, all the necessary data, including name of the customer, Credit card numbers, expiration dates, and, if requested, the digital signature of the customer and/or the facsimile of the hand-written signature of the customer to be stamped and used as described below
7. Whereas the small hand-held device requests a PIN to be actuated, and preferable, whereas the first , given, manufactures' PIN is only valid; and necessary for changing such a first PIN for a new, only know to the legitimate owner, PIN, and whereas such manufacturer's PIN is given to the person only after having checking his identity carefully once and forever, and whereas, after having changing the PIN for a new one, due to the fact that the small hand-held device allows a limited number of consecutive wrong PINs (say 3 or 10) before auto locking itself, only the legitimate owner has the capability to actuate such small hand-held device, and
8. wherever the person (the customer) would like to perform a secure Credit Card over-the-Internet transaction through a regular phone , he should use his small hand-held device, which was associated with the customer on one of the Voice –Notarial Certificator service databases, whereas the small hand-held device is able
9. to identify the authorized and legitimate device's Owner (the customer) by requesting the Personal Identification Number and
   9.1 to compute a fresh secure identification code every time the small hand-held device is actuated and
   9.2 to accept transaction data (i.e.: transaction amount, selection of the Credit Card, etc) locally entered by the customer at the time of the transaction by means of the key-pad of the small hand-held device and , preferable, to encrypt such transaction data and
   9.3 to encode this secure identification code and the encrypted transaction data to sound, whereas this sound, carrying the dynamic and secure identification code and the encrypted transaction data , is referred as the Acoustic Signature
10. and whereas the Customer places a call to an specially designed server (referred as Public VTN Client) able to interpret the customer utterances using speech recognition technologies and text-to speech technologies to read out , for the customer, Internet instructions , like the HTML ones, and use such customer's instructions as WEB- browsers instructions for browsing the Internet, and enabling to perform Internet transaction through the phone
11. whereas , eventually the customer reaches the service provider WEB site and at some time later decided to send a signed document to the service provider where such document can contain is acceptation and will to perform a Credit card transaction for a specific amount, and
12. whereas the customer sends, during the calling session, the said Acoustic Signature through the phone set's microphone, whereas this sound is converted to an electromagnetic signal at the microphone and is transmitted through the PSTN to the said special Public VTN Client server as any customer's utterance is, and

13. whereas, at the Public VTN Client server, such Acoustic Signature is digitized (i.e.: creating a file) and
14. whereas the reverse of the encoding process carried on in the small hand-held device , referred as de-encoding process (de-codification) is applied to such file containing the digitized Acoustic Signature recuperating the said dynamic and secure identification code and the encrypted transaction data and
15. whereas such string of digits referred as dynamic and secure identification code and the encrypted transaction data are encrypted and/ or Hashed , preferable, according to the standards and usage of the e-commerce Certification authorities,(whereas such encrypted string is referred here-below referred as Client Query) and whereas such Client Query is transmitted to a third party, referred here-below as the Voice-Notarial Certificator service over data lines and
16. whereas the Voice-Notarial Certificator service's Server decrypts and/or re checks the integrity and validity of the Client Query recuperating, eventually, the dynamic and secure identification code and transaction data and
17. interprets ,decrypts or re-compute and compare, the dynamic and secure identification code, identifying the specific small hand-held device and decrypts the encrypted transaction data sent
18. and whereas a database is queried in order to find out who is the owner of such small device that generated the Acoustic Signature, or in another words to whom such small device was associated with and
19. whereas once the small device owner was identified and the transaction data decrypted, the Voice Notarial Certificator Server queries a database where the Credit Card account numbers associated with such small hand-held device or/and customer are stored which can be the same said database where the small hand-held device is associated to the Owner, or a different one, and
20. whereas the Voice Notarial Certificator service queries the relevant Credit card company for obtaining authorization of the payment, directly or through a point-of sale machine, and/or through any of the companies who serves as clearing houses for Credit card transactions
21. and ,eventually , having obtained the respective authorization from the relevant credit card company
22. the Voice Notarial Certificator Server prepares a digitally signed document, with the necessary data for the complexion of the Credit Card based transaction, including name of the customer, Credit card number, amount , expiration date, and, if requested, the digital signature of the customer and/or the digital certificate generated by the Voice Transaction Notarial service, and/or the facsimile of the hand-written signature of the customer, in order to fulfill the credit card companies request of signature-on-file,
23. and whereas this document is sent to the service provider WEB-site

---

whereas this method results in a in a way of supporting phone originated transactions against a WEB site, with security.

A further variation of the method of this patent is , as above, but instead that for credit Card based transactions, for debit card and/ or Bank card based transactions.

Although the invention has been described herein in conjunction with the specified steps as set forth above, it should be clear that various modifications in the selection and arrangement of the various steps discussed herein may be made without departing from the spirit of the invention as set forth above.

Referring now specifically to the computation of the dynamic and secure Identification code at the small and hand-held device and the consequent interpretation of the Identification code, according to the method of this patent we can refer to several authentication methods , whereas all of the authentication methods are characterized by the of an transmission of an identification message consisting on 2 parts, one constant like the login name, or user name, serial number etc, and the second one referred as password, preferable variable, whereas such variable password is a sequential one, a response of a challenge sent by the Voice Transaction Notarial service, or a time stamp whereas the variable code is the result of a time based computation. All of these methods are known and in use in the market. A preferable improvement of these procedures, as presented here-below in this invention is not an authentication method but an identification one, whereas the different consists of the fact that as will be seen , the message sent according with this method has no constant part, but all of the message is variable, in order to deliver total privacy to the caller.

This invention's preferred Identification algorithm is designed to solve the 4 main problems of the Remote Transactions, namely:

1.1 Impersonation of a legitimate customer which includes:

- Interception of a true Identification Message and posterior fraudulent usage of it.
- Fabrication of a (fraudulent) Identification Message by an attacker

1.2 Repudiation of a transaction

A transaction (made by the legitimate caller), where the service provider is unable to demonstrate that, indeed, the transaction was performd by the legitimate caller.

1.3 Lack of Privacy
Lack of Privacy against eavesdroppers, mainly the capability to track the caller who uses the constant non encrypted identification, such as name, login name, serial number, etc.

1.4 Server impersonation
Server (service provider) impersonation, by an attacker, in order to steal information from the caller.

Conventional dynamic authentication schemes use a constant message in order to transmit to the server the claimed identity, and a variable / secret message (dynamic password) in order to authenticate the caller.
These schemes present the following weaknesses:

- the service provider has no defense against repudiation claims (the server knows how to compute dynamic passwords)
- the caller is trackable due to the fact that he is using a constant ID message
- in most cases the message can be intercepted and used later.

All these weaknesses are solved by this invention Identification Algorithm architecture

2.1 Start up

Due to the fact that any new system (which consists of a multitude of cards or small hand-held devices and a DECRYPTOR Server) should be a closed system, the first step to be accomplished is the System Differentiation

2.1.1 System Differentiation

A New System Administrator selects (optionally) a Third Party, independent Arbitrator. The Arbitrator and the New System Administrator select their respective SEED NUMBERS. The SEED NUMBERS will be used to initialize the Personalization Machine and the DECRYPTOR Server

More in details: the System administrator selects, preferable, 2 trusted officers.

Each of the trusted officers selects a half of the System Seed Number: a 19 digits Half System Seed Number.
This Selection and Dongles burning / writing is accomplished by means of firmware: referred as SEED SELECTION MODULE, which runs on any PC.

As a result, each half of the System Seed Number remains embedded into a respective Dongle.
The System has 2 Dongles, each one with half of the System's SEED NUMBER (19 each, total 38 hex-digits).

A parallel process of selection of a seed number is made by the Arbitrator. As a result, the Arbitrator will have 2 Dongles, each one with one half of the Arbitrator's SEED NUMBER (38 hex-digits)
Contrary to the System dangles the Arbitrator's dangles will be used to initialize the Personalization Machine only. Hence, the Decryptor Server will never know the Arbitrator Seed Numbers, and this is the basis to our claim that the Identification algorithm of this invention is non repudiable.

2.1.2 Initializing the Personalization Machine (PM):

The 4 Dangles are used to initialize the Personalization Machine (PM) in order to burn small hand-held devices for one specific system. The SEED numbers are not stored in the PM's memory, only on the PM's RAM.

2.2 Personalizing Tokens

Based on System's Seed Number, the Personalization Machine software computes and burns into the small hand-held device 4 different numbers, whereas 2 out of the 4 are System Numbers and the remaining 2 are small hand-held device specific.

These 4 numbers are respectively:

- The System Module (SM)
- The System DES key (SDK)
- The Card ID (C_ID)
- The DT0 (Random Event) whereas CTIME=GMT-DT0

This CTIME is set to the Greenwich date and time, expressed in seconds (8 hex-digits), of the encryption moment minus **DT0** (a pseudo-random number different for each device, and referred to as the Random Event). **DT0** is randomly selected by the Personalization Machine.

On the other side, based on the Arbitrator Seed Number, the Personalization Machine computes the Card Arbitrator Number (CAN). It is worth to note that the service provider's System administrator has no access to the CAN.

Therefore, 5 numbers are burned into the small hand-held device.
SM, SDK, CTIME (running number), C_ID, and CAN.

Three out the 5 are specific for the small hand-held device:

- C_ID (derived from System Seed Number)
- CAN (derived from Arb. Seed Number)
- CT (Card-Time) is incremented each second (variable)

The other 2 are System specific:

The System Modulus (SM) derived from SSN and the System's DES Key.

2.3 Computing the ID Message

The small hand-held device computes the identification message in two steps.

2.3.1 First Step, Arbitrator Related

Using the function **F_ARB**

F_ARB(CTIME,CAN) = R1

R1 is referred as the first result.
The function F_ARB can be selected for each application and does not influence the Architecture described here. The method of this invention can be use with several functions but preferable with the function F_ARB, as detailed below.

2.3.2.Second Step, System Related

Following this first result, the small hand-held device computes a second result **R2**

F_Sys_{SM} (C_ID, CTime, R1) = R2

the function **F_Sys_{SM}** can be selected for each application and does not influence the Architecture described here.

There is an additional third step which consists of the encryption of the last result using DES with a System's DES Key (**SDK**). This Step is optional, up to the System administrator decision.

This DES step has been included in order to satisfy certain Bank requirements, in view of Bank standards in use today.

Thus **$e_{DES}(R2) = R'2$**

R'2 can undergoes some permutations, addition of error correction algorithms and encoding into sound.

2.3 Interpreting a small hand-held device's Message:

The R'2 is transmitted to the Server.

At the Server the R'2 is decoded into digits, de-permutated, and Decrypted using the SDK.

$$d_{DES}(R'2) = R2$$

Then, the inverse function of F_Sys_{SM} referred as $F^{-1}\ Sys_{SM}$ is applied to **R2**

$$F^{-1}\ Sys_{SM}(R2) = C\_ID, CTime, R1$$

Having recovered the ***C_ID***, the identification is completed, while the recovery of the **CTime** authenticates it, if it falls within a predetermined tolerance window.

2.4 Arbitrating a Disputed Transaction

Assuming a specific transaction is disputed by the «legitimate caller», who claims that the transaction was not made with his small hand-held device, the System Administrator will supply the Arbitrator with the Card serial number, the transaction CTIME, and the transaction **R1** (the «supplied» R1).

The Arbitrator, using the Arbitrator. Seed Number, will compute the corresponding CAN from the Card Serial Number and then:

F_ARB(CTIME, CAN) = R1

then the Arbitrator will compare the «computed» **R1** with the «supplied» **R1**.

If both R1 are equal, the transaction was not fabricated by an imposter. Obviously, there is no way for an imposter, even for the System Administrator, to compute the correct R1 for such small hand-held device at such specific time.

2.5 Adding transaction data (locally entered)

The transaction data can be encoded, according to the method of this invention, using DES with a variable one-time key.
There are 2 preferred versions: A and B whereas

- Version A: the Transaction Data Key (TDK) is computed as a function of the C_ID and CTime
- Version B: the Transaction Data Key (TDK) is computed as a function of the CAN and Ctime

Therefore according to the method of this invention a preferable algorithm for identification consists of: the small hand-held device computes

F_ARB(CT, CAN) = R1

and

$$F\_Sys_{SM}(C\_ID, CTime, R1) = R2$$

Thus $e_{DES}(R2) = R'2$ which is the message sent.

Generating the Identification Message with the method of this invention
First step (Arbitrator related step):

It is suggested to use a Hash algorithm (like the SHA1 or any other) in the following way:

F_ARB(CTime, CAN)=HASH(CTime, CAN) = R1

Where the recommended size of CAN is more than 160 bits.

Second Step (System related step)

$$F\_Sys_{SM}(C\_ID, CTime, R1) = R2 =$$

$$[(C\_ID, CTime) \oplus C'], R1 =$$

where $C' = HASH(SM, R1) \bmod M$

And where the recommended
$M = 10,000,000,000,000,000$
And the recommended size of SM is more than 160 bits.
Actually, R2 is further DES encrypted (optional step), using a System DES Key (SDK),

$$e_{DES}(R2) = R'2$$

R'2 is encoded into sound, and transmitted.

Interpreting a Small hand-held device's Message with the method of this invention :

The Identification Server, refered as the Voice Transaction Notarial server,
1) receives R'2 and
2) knowing the System DES Key , SDK, decrypts the DES step recovering R2

R2=W,R1

3) computes HASH(SM,R1) Mod M= C'
4) compute

C' ⊕W = C' ⊕ [(*C_ID*, CTIME) ⊕ C'] =

{HASH(SM, R1) Mod M} ⊕ [(*C_ID*, CTime) ⊕ {HASH(SM, R1) Mod M}]=

(*C_ID*, CTime)

and with this, the system identifies the small hand-held device and avoids Impersonation, due to the CTime tolerance.

Arbitrating a Disputed Transaction with the method of this invention: Assuming a specific transaction is disputed by the «legitimate caller» who claims that the transaction was fabricated by the System Administrator or somebody else. The System Administrator will supply the Arbitrator with the Card serial number, the transaction CTIME, and the R1 (the «supplied» R1).
The Arbitrator will compute the corresponding CAN from the Card Serial Number (Only the arbitrator can accomplish such step, due to the need for the Arbitrator Seed Number) and then

F_ARB(CTime, CAN)=HASH(CTime, CAN) =R1

then the Arbitrator will compare the «computed» **R1** with the «supplied» **R1.**
If both R1 are equal, the transaction was not fabricated by the System administrator nor by nobody else.
Obviously, there is no way for the System Administrator to compute the correct R1 for such small hand-held device at such specific time (he does not know the CAN).

A further preferred variation of the method of this invention , for remote, Credit Card based, over-the-Internet ,transactions originated through the phone and referred as Voice-commerce transactions consists of:

1. selecting an Arbitrator, as described above, and one or several system administrators as described above
2. whereas the arbitrator can select the Arbitrator seed number , or can select trustees which can select their respective parts of such seed number, preferable according to the method described above
3. and where the system administrator also selects their respective seed number, preferable according to the method described above
4. and whereas a multitude of small hand-held devices are prepared , preferable, according to the method described above, and whereas

5. the Voice Transaction Notarial server is prepared , preferable, according to the method described above and
6. whereas for each specific customer or subscriber : issuing to each the person (the customer), which desires to perform remote Credit Card based over-the-Internet transactions from a regular phone with security, as a one time set-up procedure, a small hand-held device personalized as described above, and, obtaining from such person, an authorization to use one or several of his credit cards for paying transactions according with the procedures stated here-below, in a way that a third party, referred as the Voice –Notarial Certificator Server, will be able, upon the person request , as specified below, to stamp a digital signature on documents according with the electronic-commerce standards (e-commerce)

8 and obtaining from such customer, also, as a one time procedure, all the necessary data, including name of the customer, Credit card numbers, expiration dates, and, if requested, the digital signature of the customer and/or the facsimile of the hand-written signature of the customer to be stamped and used as described below

9 Whereas the small hand-held device requests a PIN to be actuated, and preferable, whereas the first , given, manufactures' PIN is only valid, and necessary for changing such a first PIN for a new, only know to the legitimate owner, PIN, and whereas such manufacturer's PIN is given to the person only after having checking his identity carefully once and forever, and whereas, after having changing the PIN for a new one, due to the fact that the small hand-held device allows a limited number of consecutive wrong PINs (say 3 or 10) before auto locking itself, only the legitimate owner has the capability to actuate such small hand-held device, and

10 wherever the person (the customer) would like to perform a secure Credit Card over-the-Internet transaction through a regular phone , he should use his small hand-held device, which was associated with the customer on one of the Voice –Notarial Certificator service databases, whereas the small hand-held device is able

11 to identify the authorized and legitimate device's Owner (the customer) by requesting the Personal Identification Number and

11.1 to compute a fresh secure identification code, preferable according to the method described above, every time the small hand-held device is actuated and

11.2 to accept transaction data (i.e.: transaction amount, selection of the Credit Card, etc) locally entered by the customer at the time of the transaction by means of the key-pad of the small hand-held device and , preferable, to encrypt such transaction data and

9.3 to encode this secure identification code and the encrypted transaction data to sound, whereas this sound, carrying the dynamic and secure identification code and the encrypted transaction data , is referred as the Acoustic Signature

12 and whereas the Customer places a call to an specially designed server (referred as Public VTN Client) able to interpret the customer utterances

using speech recognition technologies and text-to speech technologies to read out , for the customer, Internet instructions , like the HTML ones, and use such customer's instructions as WEB- browsers instructions for browsing the Internet, and enabling to perform Internet transaction through the phone

13 whereas , eventually the customer reaches the service provider WEB site and at some time later decided to send a signed document to the service provider where such document can contain is acceptation and will to perform a Credit card transaction for a specific amount, and

14 whereas the customer sends, during the calling session, the said Acoustic Signature through the phone set's microphone, whereas this sound is converted to an electromagnetic signal at the microphone and is transmitted through the PSTN to the said special Public VTN Client server and

15 whereas, at the Public VTN Client server, such Acoustic Signature is digitized (i.e.: creating a file) and the time of reception of such Acoustic Signature (referred as Capture Time) is registered and

16 whereas the reverse of the encoding process carried on in the small hand-held device , referred as de-encoding process (de-codification) is applied to such file containing the digitized Acoustic Signature recuperating the said dynamic and secure identification code and the encrypted transaction data and

17 whereas such string of digits referred as dynamic and secure identification code , the encrypted transaction data, and together with the time of reception of the Acoustic Signature or Capture Time, are encrypted and/ or Hashed , preferable, according to the standards and usage of the e-commerce Certification authorities,(whereas such encrypted string is referred here-below referred as Client Query) and whereas such Client Query is transmitted to a third party, referred here-below as the Voice-Notarial Certificator service over data lines and

18 whereas the Voice-Notarial Certificator service's Server decrypts and/or re checks the integrity and validity of the Client Query recuperating, eventually, the dynamic and secure identification code and transaction data and

19 whereas the server decrypts, the dynamic and secure identification code, identifying the specific small hand-held device (i.e.: recuperating the Card-ID and checking the CTime against Impersonation fraud) and decrypts the encrypted transaction data sent

20 and whereas a database is queried in order to find out who is the owner of such small device that generated the Acoustic Signature, or in another words to whom such small device was associated with and

21 whereas once the small device owner was identified and the transaction data decrypted, the Voice Notarial Certificator Server queries a database where the Credit Card account numbers associated with such small hand-held device or/and customer are stored which can be the same said database where the small hand-held device is associated to the Owner, or a different one, and

22 whereas the Voice Notarial Certificator service queries the relevant Credit card company for obtaining authorization of the payment, directly or through a

point-of sale machine, and/or through any of the companies who serves as clearing houses for Credit card transactions
23 and ,eventually , having obtained the respective authorization from the relevant credit card company
24 the Voice Notarial Certificator Server prepares a digitally signed document, with the necessary data for the complexion of the Credit Card based transaction, including name of the customer, Credit card number, amount , expiration date, and, if requested, the digital signature of the customer and/or the digital certificate generated by the Voice Transaction Notarial service, and/or the facsimile of the hand-written signature of the customer, in order to fulfill the credit card companies request of signature-on-file,
25 and whereas this document is sent to the service provider WEB-site for completing the transaction
26 and whereas if , at some time later the customer denies or repudiate the transaction, the Voice Transaction Notarial service will appeal to the Arbitrator according to the method described above, in order to show up that the transaction was made by the customer and is not a fabrication of somebody else.

whereas this method results in a in a way of supporting phone originated transactions against a WEB site, with security.

A further variation of this method is, as above, but after, or close to the moment where the small device generates the Acoustic Signature, the small device displays a variable string (referred as One-time Password) of digits and/or letters which are a mathematical function of some of the seeds or sub-seeds of the dynamic identification Code of the Acoustic Signature in a way that only such entity who can interpret the dynamic identification Code of the Acoustic Signature can compute such One-time Password , and whereas the Voice-Notarial Transaction Server computes the same said One-time Password, after having identified such small device(i.e.; decrypted the dynamic Identification Code) , and whereas the Voice-Notarial Transaction Server transmitted the said One-time Password to the service provider as data, and at the service provider the One-time Password is read out to the customer, using text to speech technologies, in order for the customer to hear the numbers and/or characters and compare with the One-time Password he reads out from the display of the small hand-held device, and , eventually , if both sets are identical, he can be sure that he speaks with the correct service provider avoiding any possibility of somebody impersonating the service provider.

A further improvement of the method of this patent is as above but whereas the One-time Password is computed by the Voice-Notarial Transaction Server , is also encrypted and or Hashed using the e-commerce standards for certification, or using the public key of the service provider as well as the private key of the

Voice-Notarial Transaction Server, in order to avoid any possible impersonation of the service provider.

Referring now to the preferred Identification algorithm described above or any other time based small hand-held device, a preferred computation of the One-time- password can be as follows:

After sending the Acoustic Signature the Small Hand-held Device computes an n HEX-digits code and displayed it on the Small hand-held device's LCD.
This code will remain in the LCD for m sec. and will disappear.
Any time the Small hand-held device holder press a button (referred as a CODE button) , the Small hand-held device will display a new One-Time -Password.
The One-Time –Password is preferable computed applying the DES algorithm to a function of CTime where the DES key is a function of the C_ID and CTime.

n-k out of the n HEX-digits are a result of this calculation. The other k, preferable k=3, are the last k digits of the CT for synchronization purposes.

The Decryption node, which can be part of the Voice-Transaction Notarial server or not, receives the Serial Number or any other identification of the Small hand-held device or any equivalent number in order to extract from the database the Card ID and can know the CTime from the Acoustic signature decryption or can extrapolate a number close to the CTime, from the Capture Time.
By means of the last k digits of the CTime, the decryption node can exactly determine the true transaction CTime
The Server can now compute the other n-K digits of the One-Time –Password applying the DES algorithm to a function of CTime where the DES key is the specific function of C_ID and CTime mentioned above.

According with a more detailed preferred implementation of the method of this invention for the computation of the One-time-password the Small hand-held device encrypts, using the D.E.S. algorithm, the result of certain (device's specific) function of the time , by using a (device's specific) key

Let assume that each device has
1-has a specific function of the time $\underline{f}n(t)=(f1,...f8)$, and
2- has a Key Kn, and
3- $e_K(a)$ means encrypting "a" by using the DES algorithm and
4- that underline $\underline{R}$ means a vector =(R1,..., Rn)
5.- t is the date and time (GMT)

$$\underline{R}=e_{Kn}(\underline{fn}(t))$$

Now the device Owner sends or write identification data like his name or the device serial number, the One-time-password and the time and date.
Therefore the authentication info , preferable consists of the time and date "t", a Serial Number (SN) and a Dynamic Code (DC) 8 characters long which is read on the token display:

$$\underline{DC} = DC1,..., DC8$$

where
DC1=R12
DC2=f6
DC3=R14
DC4=f8
DC5=R13
DC6=R16
DC7=f7
DC8=R15

The decryption Node has a database which includes for each token

SN, Kn, fn of the last transaction(referred as the parameters)

when the authentication message is received , using the Decryption Node retrieves the corresponding Kn from a database and extrapolate the $\underline{fn}(t)=f1,...,f8$ using the time of the transaction "t"
replaces f6 by DC2
replaces f7 by DC7
replaces f8 by DC4 in order to determine the exact time used by the small hand-held device for the computation of the One-Time-Password

Now the decryption Node computes

$\underline{R'}=e_{Kn}(f1,...,f8)$

and finally, compares
R'12 with DC1
R'14 with DC3
R'13 with DC5
R'16 with DC6
R'15 with DC8

Summarizing , the decryption node can recuperate, rebuild or re-compute the true One-Time -Password.

One of the application of this methodology is to avoid the server impersonation fraud as described above, but it is not the only one.
Another application of this method is the certification of the identity of the signor of any hand-written signature stamped on any document.

The application referred can be described as follows:
Assuming a person (the signor) actuate his small hand-held device, identity itself against the device by entering the correct PIN, and press the Code button. The Small hand-held device will display the One-time-password and the signor should write the One-Time-Password on the document, together with the time and date and identification information like the signor's name, login name, or serial number of the small hand-held device, or any other info which will help the Decryption Node to query the database and proceed as described above , checking the veracity and validity of such One-time-password at the presumed time of generation by the presumed small hand-held device.
Figure #1 shows a "secure check" which is a bank check graphically designed for the Signor to fill in the pertinent data such as the One-time-password which is read on the display of the small hand-held device.
Figure #2 is the print of a seal which can be stamped on any document, in order to authentify the signor by filling it in.
Figure #3 shows a document (in this a facsimile) which has been authenticated by the method presented in this invention.

US patent 5,742,684 issued to the inventor of this invention describes a possible example of the said small hand-held device.

Albeit the invention has been described herein using exemplary implementations, it should be clear that any other implementation of the methodology presented here does not represent a departure from the spirit of the invention as set forth here. The same is stated here for alterations of the sequential order of the steps or sub-steps used to explain the methodology presented.

Various modifications in the selection and arrangement of the various steps discussed herein may be made without departing from the spirit of the invention as set forth above.

We claim:

1.-A method for the identification of a first entity against a second remote entity, connected by telephone, by means of a third entity, whereas this third entity is connected by data lines to the second entity, whereas the method consists of the steps of
the use, by the first entity, of a small device able to
compute a fresh ,new identification code each time it is activated and
to encode this code into sound,

whereas each time that the first entity needs to identify itself against the second entity during a telephone call with the said second entity,

the first entity activates the small hand-held device, placed close to the telephone microphone, and whereas
the small hand-held device computes a new identification code and
encodes it into sound and
whereas this sound is transmitted through the PSTN to the second entity,

and whereas a reverse of the encoding process carried out in the small hand-held device, is applied to such sound and consequently the identification code is recovered, and is sent to the third entity as data and
whereas the third entity interprets and decrypts the identification code
identifying the specific small device held by the first entity
and whereas the result of such identification is transmitted through data lines to the second entity.

2.-A method for the identification of a first entity against a second remote entity connected by telephone, and certification of data, by means of a third entity, whereas this third entity is connected by data lines to the second entity, whereas the method consists of the steps of

the use, by the first entity, of a small device able to

compute a fresh ,new identification code each time it is activated and
to accept data, and
to encrypt such data and
to encode this code and encrypted data into sound,

whereas each time the first entity needs to identify itself against the second entity and certify data, during a telephone call with the said second entity,

the first entity activates the small hand-held device and enters the data,
whereas the device is placed close to the telephone microphone, and whereas

Fig #1

Secure Bank

John Smith
3, Palm Drive, L.A
tel: 123456789

Date _____

To _____

Amt. _____

Tele-I.D.™ Code

/1232311

Date _____

Pay to _____

US Dollars _____

Signature _____

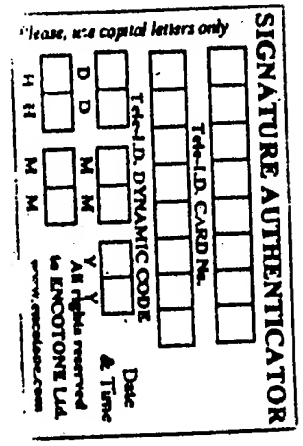
Tele-I.D.™ Code /1232311 #546878798

date: D D M M Y Y

hour: H H M M

2135464654213

Fig #2



Encotone Ltd.

FAX TRANSMITTAL

Tel. : +972 2 5866570 Fax : +972 2 5816871

To : יוליה

Company : ספיניה

Fax # : 04 - 8741429

Date : 24.9.98

From: שאול לוי

Total pages : 2
(Include this page)

Re : הערכה לחו"ל

מצ"ב הכתובת הדרושה.

S. Levy

שנה טובה/ שאול

SIGNATURE AUTHENTICATOR

Tele-I.D. CARD No. 53665701

Tele-I.D. DYNAMIC CODE 41ECF42C

Date & Time: DD 25 MM 02 YY 99 HH 11 MM 45

Please, use capital letters only

Bldg. 12, Har Hotzvim Scientific Industrial Park • P.O.B. 45031 Jerusalem 91450 Israel • Tel. 972-2-5866570 • Fax 972-2-5816871

Fig #3